UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/628,315	07/28/2000	Kazuo Ezawa	AP32610-072817.0152	3474

21003 7590 11/01/2007

BAKER BOTTS L.L.P.
30 ROCKEFELLER PLAZA
44TH FLOOR
NEW YORK, NY 10112-4498

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	

NOTIFICATION DATE	DELIVERY MODE
11/01/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

DLNYDOCKET@BAKERBOTTS.COM

mn

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/628,315
Filing Date: July 28, 2000
Appellant(s): EZAWA ET AL.

Manu J Tejwani
Reg. No. 37,952
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 23 July 2007 appealing from the Office action mailed 22 February 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is deficient. 37 CFR 41.37(c)(1)(v) requires the summary of claimed subject matter to include: (1) a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number, and to the drawing, if any, by reference characters and (2) for each independent claim involved in the appeal and for each dependent claim argued separately, every means plus function and step plus function as permitted by 35 U.S.C. 112, sixth paragraph, must be identified and the structure, material, or acts described in the specification as corresponding to each claimed function must be set forth with reference to the specification by page and line number, and to the drawing, if any, by reference characters. The brief is deficient because the Appellants has not provided a

concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner. The rejection made under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement has been withdrawn by the examiner. The Appellants have shown support for the limitation "so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device".

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,502,765	Ishiguro et al	03-1996
5,649,118	Carlisle et al	07-1997

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-44 and 46-58 are rejected under 35 U.S.C. 102(b) as being anticipated by Ishiguro et al (USP 5,502,765).

As per claim 1, Ishiguro et al teaches a method for communicating between a first portable device having a first storage device and a second portable device having a second storage device, the first storage device storing thereon a first sequence number and a first key, the second storage device storing thereon a second sequence number and a second key, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number including comparing the embedded first and second trusted times (column 16 line 11 to column 17 line 16);

performing a verification using the first and second keys (column 6 line 13 to column 7 line 59);

if the second sequence number is newer than the first sequence number by comparison of the respective embedded first and second trusted times, setting the

first sequence number to have a value of the second sequence number if the verification succeeds (column 16 line 11 to column 17 line 16); and conversely,

if the first sequence number is newer than the second sequence number by comparison of the respective embedded first and second trusted times, setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device (column 16 line 11 to column 17 line 16).

As per claims 25, Ishiguro et al teaches a portable device which is capable of performing a transaction with a further portable device, comprising:

a storage device storing a first sequence number and a first key wherein the first sequence number comprises information on a first trusted time embedded in the storage device (column 16 line 11 to column 17 line 16); and

a processing device performing the following:

receiving a second sequence number and a second key from the further portable device wherein the second sequence number comprises information on a second trusted time embedded in the portable device (column 16 line 11 to column 17 line 16),

comparing the first sequence number to the second sequence number including comparing the embedded first and second trusted times (column 16 line 11 to column 17 line 16);

performing a verification using the first and second keys (column 6 line 13 to column 7 line 59);

if the second sequence number is newer than the first sequence number by comparison of the respective embedded first and second trusted times, setting the first sequence number to have a value of the second sequence number if the verification succeeds and conversely (column 16 line 11 to column 17 line 16),

if the first sequence number is newer than the second sequence number by comparison of the respective first and second trusted times, setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device (column 16 line 11 to column 17 line 16).

As per claim 32, Ishiguro et al teaches a method for determining an approximate current time using a first portable device and a second portable device, the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number, the second storage device storing thereon a second sequence number (column 5, lines 52-53), wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number, the first sequence number being indicative of the first trusted time provided on the first portable device, the second sequence number being indicative of the second trusted time provided on the second portable device (column 16 line 11 to column 17 line 16); and

if the first trusted time is older than the second trusted time, setting the first sequence number to have a value of the second sequence number and conversely (column 16 line 11 to column 17 line 16),

if the second trusted time is older than the first trusted time, setting the second sequence number to have a value of the first sequence number so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device (column 16 line 11 to column 17 line 16).

As per claims 37, Ishiguro et al teaches a portable device which is capable of determining an approximate current time during a communication with a further portable device, comprising:

a storage device storing a first sequence number wherein the first sequence number comprises information on a first trusted time embedded in the storage device (column 16 line 11 to column 17 line 16); and

a processing device performing the following:

receives a second sequence number from the further portable device number wherein the second sequence number comprises information on a second trusted time embedded in the further portable device (column 16 line 11 to column 17 line 16),

compares the first sequence number to the second sequence number, the first sequence number being indicative of the first trusted time provided on the portable device, the second sequence number being indicative of a second time provided on the further portable device (column 16 line 11 to column 17 line 16), and executes one of the following actions:

if the first trusted time is older than the second trusted time, sets the first sequence number to have a value of the second sequence number and conversely (column 16 line 11 to column 17 line 16),

if the second trusted time is older than the first trusted time, sets the second sequence number to have a value of the first

sequence number so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device (column 16 line 11 to column 17 line 16).

As per claim 41, Ishiguro et al teaches a method for determining an approximate current time using a first portable device and a second portable device, the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number and a first key, the second storage device storing thereon a second sequence number and a second key, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices (column 5, lines 52-53), the method comprising the steps of:

comparing the first sequence number to the second sequence number, the first sequence number being indicative of the first trusted time provided on the first portable device, the second sequence number being indicative of the second trusted time provided on the second portable device (column 16 line 11 to column 17 line 16);

if the second trusted time is newer than the first trusted time, performing a verification using at least one of the first and second keys (column 16 line 11 to column 17 line 16); and

setting the first sequence number to have a value of the second sequence number if the verification succeeds and conversely (column 16 line 11 to column 17 line 16),

if the first trusted time is newer than the second trusted time, performing a verification using at least one of the first and second keys (column 16 line 11 to column 17 line 16); and

setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device (column 16 line 11 to column 17 line 16).

As per claim 54, Ishiguro et al teaches a portable device which is capable of determining an approximate current time during a communication with a further portable device, comprising:

a storage device storing a first sequence number and a first key wherein the first sequence number comprises information on a first trusted time embedded in the storage device (column 16 line 11 to column 17 line 16); and

a processing device performing the following:

receives a second sequence number and a second key from the further portable device wherein the second sequence number comprises information on a second trusted time embedded in the further portable device (column 16 line 11 to column 17 line 16),

compares the first sequence number to the second sequence number, the first sequence number being indicative of the first trusted time provided on the portable device, the second sequence number being

indicative of the second trusted time provided on the further portable device (column 16 line 11 to column 17 line 16),

if the second trusted time is newer than the first trusted time, performs a verification using the first and second keys (column 16 line 11 to column 17 line 16), and

sets the first sequence number to have a value of the second sequence number if the verification succeeds and conversely (column 16 line 11 to column 17 line 16),

if the first trusted time is newer than the second trusted time, performing a verification using at least one of the first and second keys (column 6 line 13 to column 7 line 59); and

setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device (column 16 line 11 to column 17 line 16).

As per claims 2, 31, and 58, Ishiguro et al teaches wherein the first key is a first global signing key, and the second key is a second global signing key, and wherein the verification is performed by comparing at least one first portion of the first global signing key to at least one second portion of the second global signing key (column 11 line 48 to column 12 line 7).

As per claim 3, Ishiguro et al teaches wherein the verification succeeds when the at least one first portion corresponds to the at least one second portion (column 13, line 21-32).

As per claim 5, Ishiguro et al teaches after the setting step, performing a transaction between the first card and the second card (column 19, lines 29-50).

As per claim 6, Ishiguro et al teaches if the verification fails, suspending a transaction between the first card and the second card (column 18 line 41 to column 19 line 8).

As per claims 7, 26, 48, and 55, Ishiguro et al teaches if the verification fails, recording a failure of the verification in at least one of the first storage device and the second storage device (column 18 line 41 to column 19 line 8).

As per claims 8, 27, and 58, Ishiguro et al teaches if the first sequence number and the second sequence number are equal, performing a transaction between the first card and the second card (column 19 line 29 to column 20 line 9).

As per claims 9 and 50, Ishiguro et al teaches wherein the setting step is performed by transmitting an authenticated system message ("ASM") command from the second card to the first card, and wherein at least one of the first and second cards sets the second sequence number (column 19 line 29 to column 20 line 9).

As per claims 10 and 28, Ishiguro et al teaches the first storage device stores a third sequence number thereon, wherein the second storage device stores a fourth sequence number thereon (column 15 line 9 to column 16 line 30), and further comprising the steps of: if the first sequence number and the second sequence number are equal, determining whether the third sequence number corresponds to the fourth sequence number (column 15 line 9 to column 16 line 30); and if the third sequence number does not correspond to the fourth sequence number, transmitting an authenticated system message ("ASM") command from a particular card of the

first and second cards having a newer number of the third and fourth sequence numbers to another card of the first and second cards (column 15 line 9 to column 16 line 30).

As per claim 11, Ishiguro et al teaches the ASM command is transmitted without setting the first sequence number to have the value of the second sequence number (column 15 line 9 to column 16 line 30).

As per claims 12 and 29, Ishiguro et al teaches if the third sequence number corresponds to the fourth sequence number, performing a transaction between the first card and the second card (column 15 line 9 to column 16 line 30).

As per claims 13 and 51, Ishiguro et al teaches the first key is a first global signing key, and the second key is a second global signing key, and wherein the first global signing key relates to the first sequence number, and the second global signing key relates to the second sequence number (column 16 line 11 to column 17 line 16).

As per claims 14 and 52, Ishiguro et al teaches the first key is a first global signing key, and the second key is a second global signing key, and wherein the first global signing key is associated with a first value transfer protocol ("VTP") key, and the second global signing key is associated with a second VTP key, the first VTP key being stored in the first storage device, the second VTP key being stored in the second storage device (column 16 line 11 to column 17 line 16).

As per claims 15 and 53, Ishiguro et al teaches each of the first portable device and the second portable device includes a processing device (column 5, line 42-64).

As per claim 16, Ishiguro et al teaches receiving an authenticated system message which includes a command; and executing the command (column 6, lines 7-52).

As per claim 17, Ishiguro et al teaches providing an application to at least one card of the first and second cards, the application is provided for at least one of: renewing a security feature of the at least one card, and updating a security scheme of the at least one card on-chip management (column 21 line 64 to column 22 line 43).

As per claim 18, Ishiguro et al teaches providing a reference point for time to at least one of the first and second portable devices from a central command arrangement (column 5, line 42-64).

As per claim 19, Ishiguro et al teaches enabling a selective targeting of at least one device of the first and second portable devices (column 5, line 42-64); and applying re-customization procedures on the at least one device (column 5, line 42-64).

As per claim 20, Ishiguro et al teaches selecting a particular response by the at least one device when a predetermined criteria is met (column 21 line 64 to column 22 line 43).

As per claims 21 and 42, Ishiguro et al teaches the first key is a first global signing key, and the second key is a second global signing key, and wherein the verification is performed by comparing cryptograms which are related to the first global signing key and the second global key (column 16 line 11 to column 17 line 16).

As per claim 22, Ishiguro et al teaches generating the cryptograms by one of the first portable device and the second portable device (column 16 line 11 to column 17 line 16); and verifying the cryptograms using another one of the first portable device and the second portable device (column 16 line 11 to column 17 line 16).

As per claim 23, Ishiguro et al teaches the cryptograms are generated by a central authority (column 16 line 11 to column 17 line 16).

As per claims 24, Ishiguro et al teaches after the setting step, modifying stored parameters of at least one of the first and second cards to at least one of suspend, permit, and modify subsequent operations between the first and second cards or other cards (column 15 line 37 to column 16 line 44).

As per claims 30 and 57, Ishiguro et al teaches the portable device is a smart card, and wherein the further portable device is a further smart card (column 5, line 42-64).

As per claim 33, Ishiguro et al teaches if the second time is older than the first time, setting the second sequence number to have a value of the first sequence number (column 15 line 9 to column 16 line 30).

As per claims 34 and 38, Ishiguro et al teaches after the setting step and if the first time is not equal to the second time, executing an action which is triggered by at least one of the first sequence number and the second sequence number (column 15 line 9 to column 16 line 30).

As per claim 35, Ishiguro et al teaches after the executing step and, if the first time is not equal to the second time, performing a transaction between the first card and the second card (column 15 line 9 to column 16 line 30).

As per claims 36 and 49, Ishiguro et al teaches if the first time is equal to the second time, performing a transaction between the first card and the second card (column 15 line 9 to column 16 line 30).

As per claim 39, Ishiguro et al teaches wherein the portable device is a smart card, and the further portable device is a further smart card (column 5, line 42-64), and wherein, after the execution of the particular action and if the first time is not equal to the second time, the

processing device performs a transaction between the smart card and the further smart card (column 15 line 9 to column 16 line 30).

As per claim 42, Ishiguro et al teaches wherein the first key is a first global signing key, and the second key is a second global signing key, and wherein the verification is performed by comparing at least one first portion of the first global signing key to at least one second portion of the second global signing key (column 16 line 11 to column 17 line 16).

As per claim 44, Ishiguro et al teaches wherein the verification succeeds when the at least one first portion corresponds to the at least one second portion (column 15 line 9 to column 16 line 30).

As per claim 46, Ishiguro et al teaches after the setting step, performing a transaction between the first card and the second card (column 15 line 9 to column 16 line 30).

As per claim 47, Ishiguro et al teaches if the verification fails, suspending a transaction between the first card and the second card, as discussed above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claim 4 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro et al in view of Carlisle et al (USP 5,649,118).

As per claims 4 and 45, Ishiguro et al teaches the method of encryption to secure the communication between two smart cards, as discussed above. Ishiguro et al fails to teach that the first and second global signing keys includes a private key and a public key, and wherein the verification is performed using the respective public keys. Carlisle et al teach the use of public and private keys to secure the communication using smart cards (column 8, lines 31-45). Private key cryptography is well known in the art. Private key cryptography provides a very high level of security and is implemented in many applications.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Carlisle et of within the system of Ishiguro et al because private key encryption is well established in the art and can be implemented using smart cards as taught by Carlisle et al.

(10) Response to Argument

The Appellants argue that Ishiguro does not describe or teach any such two-way mutual updating of the older time with the newer time. The Appellants submit that any teaching of updating time in Ishiguro is at most one-way (i.e. host to device). The Appellants argue that Ishiguro does not show or teach the two-way mutual updating of trusted information between two portable devices as described in claim 1.

The examiner agrees that Ishiguro does not describe or teach any two-way mutual updating of the older time with the newer time. However, independent claim has two "if-then" elements. The first "if-then" element is "if the second sequence number is newer than the first sequence number by comparison..." and the second "if-then" element is "if the first sequence number is newer than the second sequence number by comparison...". The two-way mutual updating of the older time with the newer time is recited in the second "if-then" element. The examiner asserts that only one of the "if-then" elements can be satisfied. The examiner agrees with the Appellants that the second "if-then" element is not satisfied. However, the Ishiguro reference discloses the first "if-then" element of "if the second sequence number is newer than the first sequence number by comparison of the respective embedded first and second trusted times, setting the first sequence number to have a value of the second sequence number if the verification succeeds". Ishiguro teaches in the configuration of FIGS. 1 through 3, the terminal identification number IDT, the initial value TS.sub.0 of the time stamp and the update information t set in each IC card terminal 2 are registered in the management center 4. The time stamp TS.sub.t set in the respective IC card terminal 2 is independently updated by its internal timer from the initial value TS.sub.0, for example, every day under a predetermined algorithm;

namely, the time stamp is replaced with a new time stamp in a sequential order [TS.sub.0 .fwdarw.TS.sub.1 .fwdarw.TS.sub.2 .fwdarw. . . . TS.sub.t .fwdarw. . . .], and thus the previous time stamps disappear one after another. The updating of the time stamp need not always be periodic but may also be periodic. Upon each updating of the time stamp, the number of updates (i.e. the update information or data) t is updated to t+1. Each time stamp TS.sub.t and the update information t need only to correspond to each other, that is, the time stamp may be a mere symbol and need not be a quantity.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Aravind K Moorthy AM

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

/Benjamin Lanier/
Benjamin Lanier
Examiner Art Unit 2132

Gilberto Barron Jr.
GB